UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/550,216	09/22/2005	Kei Karasawa	277747US90PCT	1366

22850 7590 04/30/2007

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/30/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/30/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/550,216	KARASAWA ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 September 2005* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/22/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for priority.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 22 September 2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 18 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Page 27, lines 21-25 defined the recording medium as being CD-ROM, a magnetic disk, or a semiconductor storage device, or a communication line. The Office's current position is that claims involving signals (i.e. communication line) encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 3-7, 13, and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0078573 to Matsuyama, hereinafter Matsuyama.

8. As per claims 1 and 13, Matsuyama teaches a packet cryptographic processing proxy apparatus (Figures 6 [block 20], 16 [blocks 20_n]) connected between the Internet (Figures 6 and 16 [block NT]) and a terminal (Figures 6 and 16 [block 10_n]), comprising:

a cryptographic communication channel information storage part which stores cryptographic communication channel information used for establishing a cryptographic communication channel at least for packet communication on the Internet (Figure 13 [step S12], paragraph 0073, i.e. the home gateway **20** holds the public key certificate PKC_G issued by the certification authority CA, and uses PKC_G to perform mutual authentication), in packet communication between a counterpart apparatus (Figures 6 and 16 [blocks 30]) connected to the Internet (Figures 6 and 16 [block NT], paragraph 0074) and the terminal (Figures 6 and 16 [block 10_n]); and

cryptographic processing means for performing cryptographic processing for a received packet based on the cryptographic communication channel information stored in said cryptographic communication channel information storage part (Figure 13 [step S12], paragraph 0073, i.e. the home gateway **20**, which is disclosed as a homer router, firewall, or bridge which all contain processing means, holds the public key certificate PKC_G issued by the certification authority CA, and uses PKC_G to perform mutual authentication).

9. Regarding claim 3, Matsuyama teaches a received packet determination part which determines whether or not a packet received from the counterpart apparatus is valid (Figures 13 [step S15], 18 [step S56], paragraphs 0101, 0151).

10. Regarding claim 4, Matsuyama teaches wherein said cryptographic communication channel information storage part includes a detachable, tamper-proof device in which at least part of the cryptographic communication channel information is stored (Figure 6 [block CA], paragraphs 0051).

11. Regarding claim 5, Matsuyama teaches wherein said cryptographic communication channel information storage part includes a storage medium in which at least part of the cryptographic communication channel information is changeable (Figure 17 [block S42], paragraph 0141, i.e. the attribute authority updating the attribute certificate stored at the gateway).

12. Regarding claim 6, Matsuyama teaches the packet cryptographic processing proxy apparatus being logically directly connected to a network interface device of the terminal (Figures 6 [blocks 10_n, 20], 16 [blocks 10_n, 20_n]).

13. Regarding claim 7, Matsuyama teaches the packet cryptographic processing proxy apparatus being implemented on a device which is connected between the Internet and the terminal and which does not have an IP address (Figures 6 [blocks 10_n, 20], 16 [blocks 10_n, 20_n],

paragraph 0073). The Examiner interprets the claim language as not having a single IP address (as implied by the singular an), and therefore can have a plurality of IP addresses. Matsuyama discloses wherein the gateway can be a router or firewall, which are known in the art to have at least two IP addresses, one for the external network and one pertaining to the internal network, and therefore teaches the claim limitation.

14. Regarding claim 18, Matsuyama teaches a readable recording medium on which a program for causing a computer to perform the packet cryptographic processing method according to any of Claims 13 to 17 is recorded (paragraph 0165).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 2, 8-12, and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsuyama in view of U.S. Patent Application Publication No. 2005/0160161 to Barrett et al., hereinafter Barrett.

17. Regarding claim 2, Matsuyama does not teach filter information storage part which stores sending source identification information, sending destination identification information, protocol information indicating a packet communication procedure and processing instruction information indicating whether or not to perform cryptographic processing, as filter information; and cryptographic processing determination means for, by referring to said filter information

storage part based on filter information in a packet received by the packet cryptographic processing apparatus, determining whether or not to perform cryptographic processing of the received packet by said cryptographic processing means based on the processing instruction information.

18. Barrett discloses the use of packet filtering, proxy applications, and screening applications to determine if a packet is authorized (paragraph 0032).

19. It would have been obvious for one of ordinary skill in the art at the time the invention was made to include filter information storage part which stores sending source identification information, sending destination identification information, protocol information indicating a packet communication procedure and processing instruction information indicating whether or not to perform cryptographic processing, as filter information; and cryptographic processing determination means for, by referring to said filter information storage part based on filter information in a packet received by the packet cryptographic processing apparatus, determining whether or not to perform cryptographic processing of the received packet by said cryptographic processing means based on the processing instruction information, since Barrett states at paragraph 0032 that using packet filters, proxy applications, and screening applications to determine if a packet is authorized would shield the target resource from unauthorized access.

20. With regards to claim 8, Matsuyama teaches a terminal information collection part which collects a part of at least one of the cryptographic communication channel information (paragraph 0073). Barrett discloses the filter information and stores the information in said filter information storage part (paragraph 0032).

21. Regarding claim 9, Matsuyama teaches a packet determination part which determines from a received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal (Figures 13 [step S15], 18 [step S56], paragraphs 0101, 0151);

a cryptographic communication channel information agreement part which, if the packet determination determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part (Figures 13 [block S16], 18 [block S57], paragraphs 0101, 0151).

22. Matsuyama does not teach a key information setting part which sets key information for performing cryptographic processing of a packet, in the cryptographic communication channel information agreed by said cryptographic communication channel information agreement part, for the terminal.

23. Barrett teaches a client device setting an encryption key to be used for secure communications (paragraph 0067).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a key information setting part which sets key information for performing cryptographic processing of a packet, in the cryptographic communication channel information agreed by said cryptographic communication channel information agreement part, for the terminal, since Barrett states at paragraph 0001 that allowing the key information to be set allows the secure connection with to be set with inherited authentication and authorization attributes

which creates a relatively simple method for establishing a secure connection with a proxy (paragraph 0007).

25. With regards to claim 10, Matsuyama teaches wherein, if determining necessity of agreement on cryptographic communication channel information, said packet determination part determines whether valid cryptographic communication channel information corresponding to the received packet is stored in said cryptographic communication channel information storage part, causes said key information setting part to set key information in the cryptographic communication channel information for the terminal if the valid cryptographic communication channel information is stored, and causes said cryptographic communication channel information agreement part to make agreement on cryptographic communication channel information if the valid cryptographic communication channel is not stored (Figures 13 [blocks S16, S17], 18 [blocks S57, S58], paragraphs 0101, 0151).

26. Concerning claim 11, Barrett teaches wherein, if said packet determination part determines necessity of agreement on the cryptographic communication channel information, and address information in the received packet is stored in said filter information storage part, said packet determination part causes agreement on the key information to be made (paragraph 0067).

27. Concerning claim 12, Barrett discloses packet filtering, proxy applications, and screening applications (paragraph 0032). The Examiner holds that acquiring address information from the

terminal and storing the acquired address information for filtering purposes is well known and commonly practiced and Official Notice of such is herein taken.

28. Regarding claim 14, Matsuyama does not teach referring to a filter information storage part based on filter information in the received packet, determining whether or not to perform cryptographic processing for the received packet; and causing the cryptographic processing to be performed if it is determined by the determination that cryptographic processing is to be performed, and causing the received packet to immediately pass or to be discarded if it is determined by the determination that cryptographic processing is not to be performed.

29. Barrett discloses the use of packet filtering, proxy applications, and screening applications to determine if a packet is authorized (paragraph 0032).

30. It would have been obvious for one of ordinary skill in the art at the time the invention was made to include a filter information storage part based on filter information in the received packet, determining whether or not to perform cryptographic processing for the received packet; and causing the cryptographic processing to be performed if it is determined by the determination that cryptographic processing is to be performed, and causing the received packet to immediately pass or to be discarded if it is determined by the determination that cryptographic processing is not to be performed, since Barrett states at paragraph 0032 that using packet filters, proxy applications, and screening applications to determine if a packet is authorized would shield the target resource from unauthorized access.

31. Regarding claim 15, Matsuyama does not teach determining whether or not a received packet requires agreement on cryptographic communication channel information and, if agreement is required, making agreement, for packet communication between a counterpart apparatus connected to the Internet and a terminal, with the counterpart apparatus on cryptographic communication channel information for performing cryptographic processing of a packet transmitted with the counterpart apparatus; setting the agreed cryptographic communication channel information for the terminal; and if agreement is not required, bypassing or discarding the received packet.

32. Barrett teaches a client device and proxy device negotiating and setting a secure communication session, for instance using an encryption key to be used for secure communications (paragraph 0067).

33. It would have been obvious to one of ordinary skill in the art at the time the invention was made to determine whether or not a received packet requires agreement on cryptographic communication channel information and, if agreement is required, making agreement, for packet communication between a counterpart apparatus connected to the Internet and a terminal, with the counterpart apparatus on cryptographic communication channel information for performing cryptographic processing of a packet transmitted with the counterpart apparatus; setting the agreed cryptographic communication channel information for the terminal; and if agreement is not required, bypassing or discarding the received packet, since Barrett states at paragraph 0001 that allowing the key information to be set allows the secure connection with to be set with inherited authentication and authorization attributes which creates a relatively simple method for establishing a secure connection with a proxy (paragraph 0007).

34. With regards to claim 16, Matsuyama teaches determining whether valid cryptographic communication channel information corresponding to the received packet is stored in the cryptographic communication channel information storage means (Figures 13 [blocks S16, S17], 18 [blocks S57, S58], paragraphs 0101, 0151).

35. Barrett teaches setting key information in the cryptographic communication channel information for the terminal (paragraph 0067); and,

if the cryptographic communication channel information is not stored, making agreement on the cryptographic communication channel information, storing the agreed cryptographic communication channel information in the cryptographic communication channel information storage part as well as setting the agreed cryptographic communication channel information for the terminal (paragraph 0067).

36. Concerning claim 17, Barrett teaches if agreement on cryptographic communication channel information for the packet is required, determining first whether address information in the received packet is stored in a filter information storage part; and, if the address information is stored, performing the determination about whether valid cryptographic communication channel information is stored in the cryptographic communication channel information storage part (paragraph 0032, i.e. packet filtering).

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

38. The following patents are cited to further show the state of the art with respect to secure proxies, such as:

United States Patent Application Publication No. 2005/0015462 to Lee et al., which is cited to show a service gateway for authenticating a client's requests to access services beyond the gateway.

United States Patent Application Publication No. 2004/0158712 to Lee et al., which is cited to show managing access to non-free multimedia in an intranet.

United States Patent Application Publication No. 2005/0210072 to Bojinov et al., which is cited to show a file system proxy's performance and security features.

United States Patent Application Publication No. 2003/0009597 to Joung, which is cited to show a web server proxy agent for fetching information on an appliance connected to a home network.

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

40. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

41. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf